UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF NEW YORK

State of New York, *et al.* *Plaintiffs*, *v.* U.S. Department of the Treasury, *et. al.* *Defendants*.	Case No. 1:25-cv-1144-JAV

I, Joseph Gioeli III, declare under penalty of perjury:

1. I currently serve as the Deputy Commissioner for Transformation and Modernization in the Bureau of the Fiscal Service (Bureau or BFS), in the U.S. Department of the Treasury (Treasury), and have been employed in this role since 2023.
2. In my current role, I oversee, among other things, the Bureau's Office of Information and Security Services (ISS). ISS promotes the integrity and operational efficiency of the federal government's financial infrastructure that is within Treasury's responsibility, while ensuring the security of that infrastructure and the information it contains. In my position, I also oversee the Chief Information Officer, who has authority over the security of and access to these systems. I have extensive knowledge of the Bureau's technology investments, as well as the related technology and cybersecurity strategies that support our enterprises. I am also familiar with Bureau requirements around access to sensitive systems, including the typically required vetting and IT Security training protocols. I provide this declaration in support of the Defendants' Motion to Partially Dissolve the Preliminary Injunction. I also below provide a correction to a fact I provided in my earlier declaration filed in this case.

3. **Vetting/Background Investigations**: To ensure that the Bureau manages its personnel consistent with national-security and public-trust interests, all employees and non-employees conducting work for or on behalf of the Bureau, or on Bureau systems, undergo vetting and background investigation, before receiving Bureau authorization to begin employment and/or work. This vetting is coordinated through the Treasury Department's Office of Security Programs, as further discussed in the accompanying Declaration of Kari Mencl.
4. If an individual is employed by another agency or organization—including the Treasury Departmental Offices (*i.e.*, Main Treasury)—Bureau security personnel will, prior to granting that person access to Bureau data or systems, obtain assurance from that agency or organization that appropriate vetting and background investigation of the individual has occurred there. For an employee of the Treasury Departmental Offices, Bureau security personnel typically will rely on that assurance, and will not undertake any additional vetting or background investigation on their own.
5. On or about January 22, 2025, Bureau security staff obtained assurance from the Treasury Office of Security Programs (TOSP) that TOSP had vetted Tom Krause for onboarding as a Treasury employee.
6. On or about February 19, 2025, Bureau security staff obtained assurance from the Treasury Office of Security Programs (TOSP) that TOSP had vetted Ryan Wunderly for onboarding as a Treasury employee.
7. Computer systems access can take the form of physical access, logical access, and what is often referred to as over-the-shoulder access. A computer-system user has physical access when they can physically touch the computer system's hardware (mouse, keyboard, etc.).

8. Logical access is the permission given to users to access specific parts of a computer system or software. The details of a user's logical access determine what the user can do, and can be controlled using passwords or Personal Identity Verification (PIV) cards. For example, an employee's logical access might allow him or her to access certain files or programs, but not the entire network.

9. An individual with over-the-shoulder access is authorized to view a computer system while in physical proximity (or virtual proximity, such as through screen-sharing) with another person who has logical access and permissions. Over-the-shoulder access, alone, is not considered logical access.

10. **Basic IT Security Trainings**: All Bureau employees and contractors who have been granted logical access to any Bureau computer system (i.e., permission given to users to access specific parts of a computer system or software) are required, within 60 days of gaining that access, (and then annually) to complete the following Information Technology (IT) Security training (collectively "IT Security Training"):

    - **Cybersecurity Awareness**, which educates employees about typical threats to Bureau computer systems (phishing, for example) and covers cybersecurity best practices for mitigating such threats (spotting phishing emails, for example);
    - **Fundamentals of Records Management**, which educates employees about document/records-retention/disposal requirements and practices;
    - **Fiscal Service Security Rules of Behavior**, a document spelling out the responsibilities and procedures for the secure use of Bureau data, equipment, IT systems, and facilities;

- **Safeguarding Federal Tax Information**, which educates employees about the requirements for handling federal tax information, including the disclosure requirements under the Internal Revenue Service Code, 26 U.S.C. § 6103; and
- **Treasury Insider Threat Awareness**, which educates employees about detecting and reporting attempts by fellow employees or contractors to illegally obtain classified, confidential, or sensitive agency information; recruitment by foreign-intelligence services; and otherwise avoiding the dissemination or mishandling of sensitive information.

11. Non-Bureau employees, including employees of the U.S. Treasury Department (Main Treasury) or employees of other federal agencies are also required to complete IT Security Training within 60 days of gaining logical access to Bureau computer systems. Typically, such employees will have completed one or more of the IT Security Training courses/modules at their home agency, which do not need to be repeated at BFS.
12. Due to the short duration of his employment at the Treasury, Marko Elez did not complete any of the trainings discussed above, although he did receive logical access to certain BFS systems. The access that Mr. Elez was provided to these payment systems did not require a security clearance.
13. Currently, and to the best of my knowledge, no Treasury DOGE Team Members are Bureau employees, and none have logical access to any Bureau computer systems.
14. **Specific Payment System Trainings**: Because access to any of the Bureau's payments systems constitutes logical access, an individual with access to any such systems must complete the IT Security training described above within 60 days. Based on information

provided by the Bureau's Federal Disbursement Services Organization, additional training requirements are required for those assigned to particular "roles" within particular payment systems. For example, those who are assigned to a PAM-related "information-production" role require additional training in the form of hands-on training with a more experienced user, and the study of written materials including the PAM Operations Processing Procedures Manual; those assigned to an "auditing" role in SPS require additional hands-on training from a manager or peer with expertise and review of a user guide; those assigned to an "information-gathering" role in ITS.gov must take ITS.gov User Training conducted by the Bureau's Diversified Payment Services Division. Additional roles require other additional trainings.

15. Marko Elez was never assigned a payment-system role that required any additional training, and did not complete any such additional training.

16. **Correction:** On February 11, 2025, I executed a declaration, docketed with this Court in this case as ECF No. 34. In paragraph 19 of that declaration, I stated that "Mr. Elez never logged into ASAP, CARS, or ITS.gov, as technical access to those systems was never established for him."

17. I wish to make a correction to the last part of this statement. I have very recently learned, from the Bureau's Fiscal Accounting unit, that Mr. Elez did receive the ability to access the CARS Application leveraging a read-only auditor role, a role that did not require additional training. Further analysis is underway to ascertain whether he ever accessed this system, but so far, neither I nor personnel in my unit have not found any records indicating that he did. I apologize to the Court for the inadvertent error.

18. **Mitigation Measures**: My February 11, 2025, declaration, ECF No. 34, describes mitigation procedures that the Bureau implemented with respect to Mr. Elez. As described in my prior declaration, those mitigation measures included requiring Mr. Elez to access BFS systems through his BFS laptop only; using cybersecurity tools to monitor his usage of the laptop; engaging enhanced monitoring and protective measures, including blocking the ability to use external peripherals, data exfiltration detection, and encryption; providing "read-only" access, and requiring reviews to be conducted in low-utilization periods to minimize disruptions; limiting the access to Mr. Elez only, as the single "technical team" member; agreeing to provide safeguarding and handling instructions; and creating the secure code repository, or "sandbox" which allowed Mr. Elez to securely access and explore source code outside the production environment. *See* ECF. No. 34 ¶¶ 12-16.

19. Currently, no Treasury DOGE Team Members have logical access to Bureau payment systems. If/when any Treasury DOGE Team Members gain such access, the Bureau will implement the same mitigation procedures outlined in my declaration, ECF No. 34, as well as any other appropriate mitigation procedures. These employees will also be required to comply with the vetting and training requirements described above.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 3/4/25

Signed: [signature]

Joseph Gioeli III
Deputy Commissioner of Transformation and Modernization
Bureau of the Fiscal Service
United States Department of the Treasury